

09/321611

A non-iterative technique for calculating the remainder of modulo division, which requires significantly fewer operations than the traditional iterative technique for the same calculation. The number of calculations ^{required} requires in the present invention is independent of the number of bits of the divisor in the modulo operation. Two requirements of the non-

5 iterative technique are that the value of the divisor D should be equal to $2^n - 1$ (where n is
the number of bits of the divisor D) and the value of the dividend N should be less than or
equal to $(D-1)^2$, but ^{greater} ~~great~~ than or equal to zero. If these two conditions are met, the
10 remainder R of $M \bmod D$ is determined by summing the upper $\lceil \frac{n}{2} \rceil$ and lower $\lfloor \frac{n}{2} \rfloor$ bits of the
11 dividend N.

② T, 0010
② T, 0011

[illegible]